Development of a Standardized Testing Environment for QRNGs based on Semiconductor Laser Phase Noise

Matthias Ostner,* Innocenzo De Marco,† and Christian Roubal‡
German Aerospace Center (DLR)
Institute of Communications and Navigation
Münchener Str. 20, D-82234 Weßling, Germany

(Dated: July 24, 2025)

Quantum random number generators (QRNGs) based on semiconductor laser phase noise are an inexpensive and efficient resource for true random numbers. Commercially available technology allows for designing QRNG setups tailored to specific use cases. However, it is important to constantly monitor whether the QRNG is performing according to the desired security standards in terms of independence and uniform distribution of the generated numbers. This is especially important in cryptographic applications. This paper presents a standardized test scheme that helps to assess the acceptable operating conditions of a semiconductor laser for QRNG operation, using commonly accessible methods. This can be used for system monitoring, but crucially also to help the user choose the laser diode which better suits their needs. Two specific quality measurements, ensuring proper operation of the device, are explained and discussed. Setup-specific approaches for setting an acceptance boundary for these measures are presented and exemplary measurement data showing their effectiveness is given. By following the comprehensible procedure described here, a QRNG test environment tailored to specific security requirements can be reproduced.

I. INTRODUCTION

Random numbers are essential for various modern applications, with differing requirements based on context. In quantum key distribution, the aim is to produce independent and identically distributed (IID) numbers, ensuring that the random number outputs are uncorrelated and show uniform probability distribution across the space of potential outputs [1, 2]. Quantum random number generators (QRNGs) utilize random quantum phenomena, such as the detection of single photons after they pass through a beamsplitter, as their entropy source, aligning with the probabilistic principles of quantum theory [3, 4]. QRNG technology as a whole has advanced significantly, and its applications are now expanding beyond quantum communication domains. It's no longer confined to its main application being a subsystem to quantum key distribution devices, but is now being utilized in various sectors of the general market, with QRNG chips being installed in smartphones and self-driving vehicles to improve their security against external attackers.

A fast and effective type of QRNG is based on phase fluctuations in gain-switched semiconductor lasers, originally presented by Jofre et al. in [5]. The general idea behind this approach is that when the photon density in the laser medium is low, e.g. when the laser is switched off, spontaneously emitted photons randomize the phase of the cavity field and this phase randomization leads to random interference intensities of subsequent pulses emitted in the lasing phases of the gain-switched laser. This interference is achieved with an asymmetric Mach-Zehnder-Interferometer (aMZI).

QRNGs based on this concept have been extensively studied and developed. Since the first demonstration in 2011 [5], major improvements have been made. In particular, much work has been done to improve the key rates [6], miniaturize the optical systems [7–9], and develop new hardware and software-based post-processing techniques to enable real-time processing and generation [10, 11].

The model developed by Henry et al. [12] describes the cavity field phase diffusion due to spontaneous emission leading to a Gaussian-like phase distribution between subsequent pulses. Since for interference intensities only relative phase values between $[-\pi, \pi]$ are relevant, the Gaussian phase distribution gets projected onto this interval and produces a uniform phase distribution across it, after typical off-times in the order of 10^{-10} s [13]. This limits the pulse repetition frequency to a few GHz and therefore also the random number generation rate.

The interference intensities caused by a uniform underlying phase distribution are not uniformly distributed but describe an arcsine distribution due to the cosine-dependence of the interference intensity. This is visualized in Figure 1. As the resulting intensity values are not uniform, one needs to perform a randomness extraction step in order to get a close-to-uniform distribution of the QRNG output numbers. There are several extraction methods suitable for cryptographic applications, one example is the seeded Toeplitz extractor [14] which reduces the bit length of each output but thereby increases the uniformity of the distribution and decreases the amount of cryptographically insecure numbers to a point sufficient for the specific requirements of a given application. This last step is not treated in this paper, so other sources can be considered for more detail, e.g. [15].

* matthias.ostner@tum.de
† innocenzo.demarco@dlr.de
‡ christian.roubal@dlr.de

The design and experimental realization of such a QRNG, as outlined in Section II, is comparatively straightforward. Utilizing a custom-made setup allows customization to specific security requirements, enhancing trustworthiness and minimizing dependence on external manufacturers, while also potentially optimizing system design by conserving resources such as weight, space, or power.

However, there are complications to be aware of. Although the entropy source of such devices is based on unpredictable quantum processes, which makes them ideal for true random number generation, potentially predictable classical noise influences the outputs of these generators, especially in the measurement and digitization steps of the procedure, but also in the optical output due to effects like jitter and chirping [16]. Randomization of the output can also be hindered by backreflection of light into the laser cavity [17] or by attacks on these devices e.g. by injecting electrical signals into the measurement stage through RF antennas [18]. Therefore, a requirement for secure generation of random numbers is that the used device can be trusted and that the user is aware of the various sources of noise influencing the QRNG output. This requires a testing framework for the QRNG to make sure that the QRNG is performing according to the defined requirements. Examples of approaches to increase the security of a QRNG via the Min-Entropy formulation exist and can be found e.g. in [19] and [20]. However, gaining the necessary detailed knowledge about classical contributions and incorporating it into the randomness extraction procedure can be experimentally and mathematically challenging and time-consuming.

An easier approach towards QRNG quality assurance is presented in this paper. The goal of this work is not to quantify how much information can be retrieved from raw intensity values but to propose a simpler qualification procedure that allows for discriminating between operating conditions that allow for QRNG operation and ones that don't. This proves useful in monitoring the performance of a running QRNG, similar to previously reported work [9], but crucially it also provides a full qualification framework to assess whether or not a laser is suitable to be used as a QRNG in the first place, which to our knowledge has never been fully laid out.

In the following, a comprehensive and transparent framework consisting of two quantitative quality measures is presented. Our framework allows for easy implementation in various circumstances. An exemplary set of boundary conditions is given to ensure independence of the generated random numbers and the uniformity of the underlying phase distribution, the preconditions for IID number generation. Furthermore, methodological requirements and risks are explored. Finally, experimental data is presented which proves the applicability of the defined test procedure.

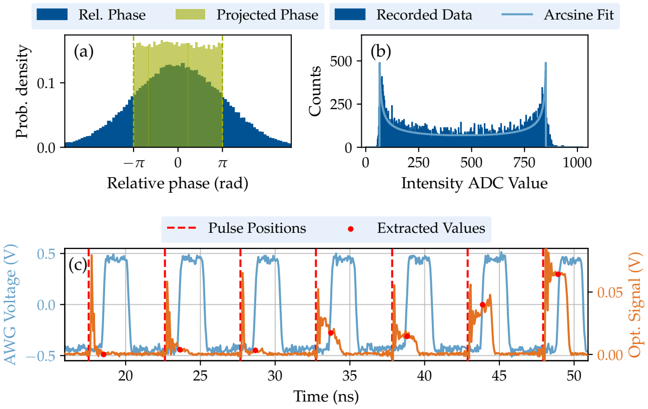

FIG. 1. (a) A Gaussian distribution of the relative phase between two subsequent laser pulses evolves through phase diffusion. Projected to the phase space relevant for interference, it gives a uniform distribution after some time. (b) A recorded pulse intensity histogram and a fitted ideal arcsine distribution resulting from perfect phase randomization. (c) Electrical and optical pulse trace detail recorded with the described setup. The automatically extracted intensity values are marked with red dots and contribute to the intensity distribution above.

II. EXPERIMENTAL QRNG SETUP

The setup for the custom QRNG evaluated in this manuscript is similar to the one originally proposed by Jofre et al. [5] and consists of a gain-switched semiconductor laser module connected to a fiber-based aMZI. The current pulses driving the laser consist of a constant bias current from the laser driver and a superimposed square signal from a 6 GS/s arbitrary waveform generator (AWG). The produced light pulse train interferes with a copy of itself delayed by $\Delta\tau$ and the interference intensity is measured with a 50 GHz photodetector and an oscilloscope with a bandwidth of 8 GHz and an ADC with 10 bits of vertical resolution. The measured intensities are recorded as a raw string of random bits. The acquisition of one intensity value per pulse is triggered by the AWG pulses combined with a measured delay between the electrical and optical pulses. Three laser models from different manufacturers were scrutinized as QRNG sources and 5000 different operating parameters per laser were evaluated for their ability to generate quantum random numbers according to the two criteria explained in sections III A and III B. All of them are DFB lasers with a center wavelength around 1550 nm. For each parameter set, 10000 pulses were recorded and the intensity values were evaluated with both criteria for their suitability for QRNG application. The varied driving parameters were the chip temperature T, the duty cycle DC of the pulses, the pulse peak current I_m, and the composition of the pulses determined by a modulation depth parameter MD determining how high the constant bias current and the modulation signal amplitude were. When MD surpasses

0.5, the modulation signal amplitude is greater than the constant bias so that reverse biasing is achieved in the off-phases of the lasers.

The used aMZI was built by splicing two fiber-based 50/50 couplers together, with one arm being 1 m longer than the other, resulting in a delay of $\Delta\tau = (5.0678 \pm 0.0584)$ ns. This delay corresponds to an ideal pulse repetition frequency of 197.32 MHz leading to perfect overlap of the pulses. An average splitting ratio of 51.50/48.50 ±2.56 was measured. The aMZI is a very important component in this system and it was designed to match the application requirements. In this case the AWG sample rate defined the necessary delay.

The system phase noise was measured under various laser operating conditions with three different, commercially available laser types. The reason for using different lasers is to compare their behavior and quality which is presented in Appendix A. Driving the lasers in CW mode, the intensity fluctuation was measured in 5 ns steps and converted to phase noise values. The worst-case gave a Gaussian phase-noise distribution between two positions with a width of $\sigma = (36.33 \pm 0.41)^\circ$ which constitutes substantial phase noise. However, it is far from being strong enough to give a uniform distribution across the whole interval $[-\pi, \pi]$, which is sufficient to distinguish between driving conditions that enable phase randomization caused by spontaneous emission and such that don't. Therefore, the setup is suitable to investigate the QRNG quality measures introduced in Chapter III.

III. QUANTITATIVE DECISION RULES FOR QRNG OPERATION

In order to qualify certain laser operating conditions as phase randomizing and therefore suitable for quantum random number generation, quantitative analyses of the system and the measurement results are needed. There are concepts how to approach this task. One is a Min-Entropy formulation to estimate how much quantum randomness can be extracted from the numbers obtained. The most basic formulation of the Min-Entropy is

$$H_{min}(X) = -\log_2 \big(\max_{1\leq i\leq k} p_i \big), \tag{1}$$

where $X = \{x_1, x_2, ..., x_k\}$ is a discrete random variable and p_i is the probability of outcome x_i. This measure gives the target bit length at the end of the final extraction process. Depending on the imbalance in the initial intensity distribution, more or less information can be obtained where the maximum is achievable with a perfectly uniform distribution $p_i = 1/k$. This formulation is used e.g. in [21] as a QRNG quality measure but it does not take into account that classical noise contributes to the measurement and broadens the underlying phase distribution so that the phase drift is not only caused by quantum processes. This lowers the security of the obtained random numbers. Also, when the classical noise smears out the arcsine distribution, the Min-Entropy increases although one can tell less about the underlying phase distribution. One approach to solve this issue is to adapt the Min-Entropy formulation towards a conditional Min-Entropy requiring detailed knowledge about the system components. This is done in detail in [15, 20] and applied for example in [19]. Getting this knowledge about the individual noise contributions is a laborious task, especially when environmental circumstances vary. In order to overcome the weaknesses of the Min-Entropy formulation and find a more practical way to the qualification of QRNGs based on the concept described, an approach via the statistical distance is described in Section III A to qualify sufficient close-to-uniform phase randomization or identical distribution. There still is the need to know the overall noise in the detection system, but measuring this is less complex compared to an estimation for each individual source of noise. In order to test a QRNG output for independence of the outcomes, additionally, an autocorrelation criterion is presented. These two criteria together, if applied correctly, constitute a simple testing environment for QRNGs generating IID numbers.

A. Statistical Distance

The first criterion mentioned is the statistical distance between the measured intensity histogram $I = \{n_0, n_1, \ldots, n_{1023}\}$ and a fitted arcsine distribution $A = \{a_1, a_2, \ldots, a_{1023}\}$. The n_i indicate the number of intensity measurements at the ADC value i between 0 and 1023 and the a_i represent the expected measurements in the respective ADC bin in the case of an ideal arcsine distribution. The quantity is assumed to be suitable as it quantifies the underlying phase uniformity by inferring it from the closeness between the measured intensity histogram and the ideal one that would follow from a uniform underlying phase. The value is calculated as follows:

$$d_{stat} = \frac{1}{2N_I} \sum_{i=0}^{1023} |a_i - n_i| \tag{2}$$

The center value of each arcsine bin should be taken so that there is no divergence at the boundaries of the definition range. For each measurement, $N_I = \sum_{i=0}^{1023} n_i$ is the overall amount of intensities measured in one run. It holds that $N_I = \sum_{i=0}^{1023} a_i$, so for the fitting of the arcsine distribution the area under the arcsine corresponds to the total amount of measurements taken. In the actual experiment, the statistical distance is measured by recording an intensity histogram and fitting an ideal arcsine with the same area as the actual distribution to it while minimizing the statistical distance.

In [9], the statistical distance, or total variation distance as they call it, was already used to monitor their QRNG performance. The difference in the approach is that they evaluated the statistical distance between a current distribution and an initially recorded reference distribution. In our approach, the ideal arcsine is fitted to minimize the distance to a given intensity distribution. This makes the approach more robust against changes in the ADC dynamic range fraction used by the recorded intensities, which might be caused e.g. by a varying laser output power. Additionally, there is no previously recorded histogram, which needs to be qualified in the first place, necessary to qualify the measured histograms but a numerical approach can be taken to define the boundary for the criterion.

For that, the phase diffusion width σ_Φ necessary for a certain application has to be determined. Then, with that width, the intensity output of interference measurements can be simulated. The system's overall noise needs to be measured and convolved with the generated histogram. Finally, fitting the arcsine with minimal statistical distance gives the boundary value for the QRNG below which one can accept the operating conditions. The main advantage of this approach is that it is easier to implement than the detailed Min-Entropy adaptions mentioned above.

Determining the minimum width of the phase drift distribution between two pulses is more or less arbitrary and depends on the security of the random numbers that is desired. A study of the connection between security in QKD protocols and phase drift width is found in [22] together with numerical examples. A trade-off between security and pulse generation frequency, so QRNG speed, has to be made as a wider phase drift is achieved by longer off-times of the laser. More precisely, the phase drift width is linearly proportional ($\sigma_\Phi^2 \propto t$) to the elapsed time according to theory [12]. A reasonable threshold for the Gaussian phase distribution width was estimated in [13] to be $\sigma_\Phi^2 = (0.8\pi)^2$ and taken as the goal in this study. Given the relative phase noise σ_Φ of the used setup described above, the target phase drift is increased to $\sigma_\Phi^2 = (0.825\pi)^2$, in order to guarantee that the actual quantum phase drift is exceeding the threshold.

In a next step, an ideal arcsine was fitted to the generated histogram, and the statistical distance was calculated. This was done for different values of the intensity noise and for different fractions of the recorded intensity values within the dynamic range of the ADC. In the experiment, different dynamic range settings had to be used, as the varied driving current led to varying intensity output. In the selected range of settings, the intensity noise of the detection system was measured and found to be in the range of (0.43-3.0) % of the maximum intensity at that setting. As the oscilloscope range cannot be set in arbitrarily fine steps, the measured intensities usually do not cover the whole ADC range, instead they typically take up (50-85) %.

These two parameters, the noise and the ADC fraction, were scanned with the above procedure and a mean statistical distance of $d_{mean} = 0.155$ was found. For increasing noise and intensity fraction, the statistical distance obtained seems to increase almost linearly as seen in Figure 2. The increase with noise is desirable, as this, contrary to the increase of the Min-Entropy, leads to a rejection of generated numbers if the intensity distribution is so different from an arcsine that one cannot infer a sufficient underlying phase randomization.

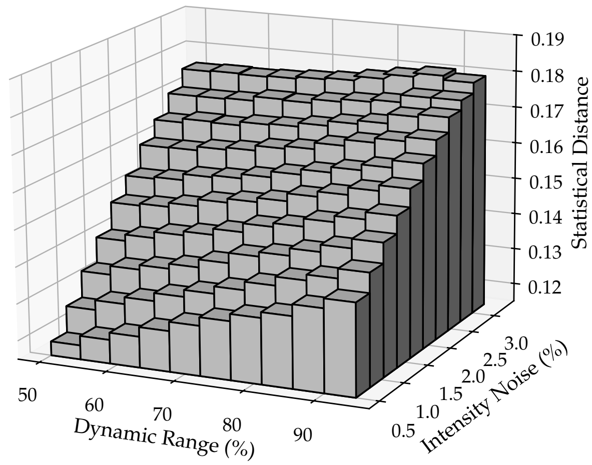

FIG. 2. Simulated statistical distance for varying ADC dynamic range fractions taken by the recorded intensity values and varying intensity noise in the system in percent of the ADC range. There is monotonous dependence of the statistical distance with respect to both quantities. The mean $d_{stat} = 0.155$ serves as the boundary.

For the measurement results presented in this work, the mean simulated statistical distance $d_{mean} = 0.155$ was chosen as the boundary condition so that this criterion is assumed to be fulfilled if $d_{stat} \leq d_{mean}$.

Regarding this numerical approach it is important that it reflects the sampling strategy of the actual verification measurements in terms of sample size. In Figure 3 one can see that for identical values of noise and ADC dynamic range the statistical distance varies for varying sample sizes and eventually converges. One should be aware of that behavior and perform the boundary estimation with the same parameters as the actual qualification measurements. One should also be aware that the standard deviation of the statistical distance measurements depends on this sample size. In the same figure the exponential decrease in fluctuations with increased sample size is shown. This is something to be aware of when doing the trade-off between sampling speed and accuracy of the measurements.

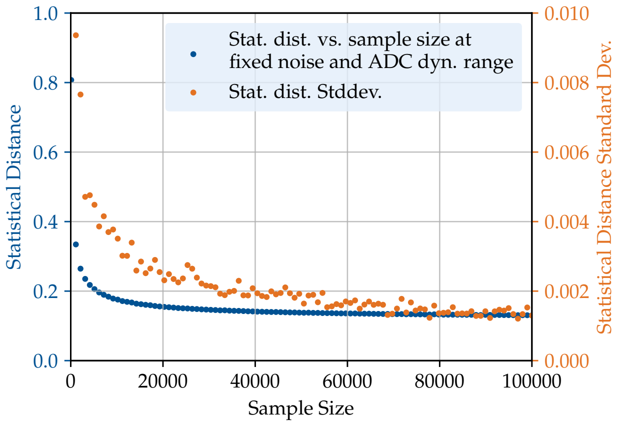

FIG. 3. Simulated Statistical distance and its standard deviation at a fixed noise value of 1.5 % and an assumed ADC dynamic range fraction of 50 %. With increasing sample size, both values decrease and converge. This emphasizes that simulations have to match the experimental conditions.

B. Autocorrelation

Besides the criterion for the statistical distance, another important quantity was chosen to qualify the randomness of the extracted pulse intensities and therefore the generated random numbers. This quantity is the autocorrelation Γ_d of the sequence of N_I extracted numbers X_i,

$$\Gamma_d = \frac{1}{N_I} \sum_{i=1}^{N_I} X_i \cdot X_{i+d} - \overline{X}^2. \tag{3}$$

The autocorrelation is a measure of how similar the sequence of random numbers is to a shifted version of itself. If the autocorrelation for a certain shift is high, information about later numbers can be gained by knowing previous ones which makes them predictable. High autocorrelation values can therefore disqualify the independence of generated random numbers. Vice versa, a low enough autocorrelation is an indicator for independence of the QRNG output. To compare the autocorrelations for different signals, one can calculate a normalized autocorrelation coefficient [23] $C_d = \frac{\Gamma_d}{\Gamma_0}$. This coefficient will take a value between $[-1, 1]$. In this formalism, $C_0 = 1$ is always true and this value is the reference for the absolute values of the autocorrelation coefficients given in dB from here on.

For a random signal, a rapid drop of the autocorrelation coefficient is expected and necessary already for low shifts. For the experiment in which the laser parameter space is explored, the autocorrelation coefficient value for $d = 1$ is taken as the second criterion to qualify certain operating conditions as phase randomized. As in the case of the statistical distance, a boundary value can also be chosen for the autocorrelation, above which a string of random numbers is rejected. This boundary should be chosen adequately for a given need of security in a specific application. For this analysis, a boundary was defined by measuring the autocorrelation coefficient for $d = 1$ for intensity values obtained from CW operation of the lasers above threshold with the interferometer connected.

The measured coefficients for different settings and laser models ranged from (-15.42 ± 0.10) dB to (-0.70 ± 0.01) dB. This means that if the extracted random numbers in gain-switching mode show a lower C_1 than -15.52 dB, they are more independent than the numbers extracted from CW light with superimposed noise. The boundary on the autocorrelation coefficient C_1 for the demonstration measurements was chosen to be $C_1 \leq -18.52$ dB, so half the CW value. This boundary was used as the conducted measurements should demonstrate the identification of QRNG operation. Achieving a higher independence of the outcomes than that produced by non gain-switching operation is sufficient in this case.

It should be noted that this choice only suits this application. In a real application, the boundary condition should be chosen so that the security needs are matched. Furthermore, taking into account the higher autocorrelation coefficients C_i with $i > 1$ is advisable in order to improve the protection against attacks like the one described in [18], where RF signals were injected into the measurement setup, or device failures. In the lab setting none of these concerns were relevant and measuring the first 10 autocorrelation coefficients for a certain laser setting producing gain-switching conditions showed that in the case of randomization, the coefficient means do not decrease further when increasing the index i. For non-randomizing conditions they do. This agrees with the assumptions about the autocorrelation behavior with respect to different levels of coherence between the pulses. A comparison between different operating conditions is presented in Figure 4.

When comparing the autocorrelation measurements with rate equation model simulations of the experiment, an initial discrepancy appeared. When the model did not contain a slow phase drift present in the actual setup, the autocorrelation values were underestimated in the simulation model under non-gain-switching conditions. This lead to the acceptance of parameters which were excluded in the actual experiment because they did not enable gain-switching and therefore sufficient phase randomization. Because of the used form of the autocorrelation coefficients, shown in equation (3), even very stable pulse intensities showing a high autocorrelation can give low coefficients if the variation of the pulse intensities around their mean is very small. Then, the autocorrelation coefficients are sensitive to small variations in pulse intensity leading to results not compatible with the defined boundary. In order to avoid a misbehavior in actual use of the criterion, one has to make sure that the boundary value is actually determined with the used QRNG setup so that all factors influencing its behavior are taken into

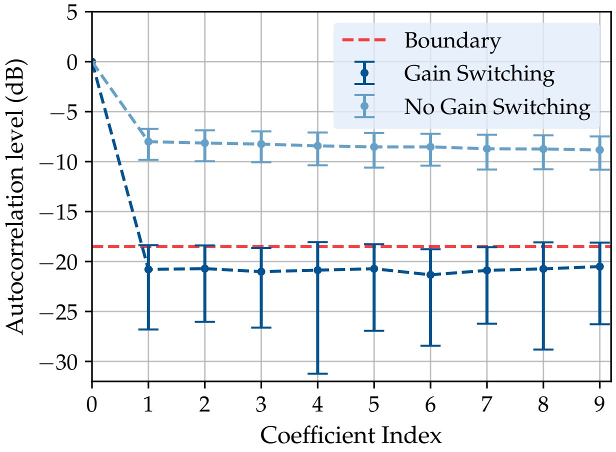

FIG. 4. Measured autocorrelation coefficients C_i and deviations under QRNG and non-gain-switching conditions. Both datasets were recorded with Laser 3. In QRNG operation, the coefficients are below the boundary and do not decrease with increasing index i. Under non-gain-switching conditions, the means decrease at higher indices.

account. A second way would be to adapt the definition of the autocorrelation, e.g. by using the ADC range median as a static mean or by normalizing the autocorrelation with the range of obtained intensity values. Both adaptations were not tested, but they are mentioned as ideas if the definition given here should not be suitable to the reader's device properties.

IV. VALIDATION MEASUREMENTS

The suggested criteria were tested by validating the three lasers mentioned in II for QRNG operation through a series of measurements. The lasers' operating parameter ranges explored both gain-switching and non-gain-switching operation, in order to fully analyse the boundary conditions between random and non-random generation. This set of measurements works as an exclusion and selection criterion: when developing a QRNG, it is important to select the right components. Lasers which do not show a wide enough operating window, based on these measurements, cannot be trusted for effectively generating quantum random numbers, and so they should not be used. The width of the boundary conditions can be adjusted depending on individual security requirements.

An exemplary plane in the four-dimensional parameter space explored for Laser 3 is shown in Figure 6. The plot shows that the both the statistical distance and the autocorrelation criteria with their respective boundaries distinguish between parameters that allow for QRNG operation and those that don't, which is their main purpose. From analyzing this plane, one can make multiple observations confirming that they reflect expected QRNG behavior and monitor the QRNG performance. Most importantly, there are operating conditions expected to be rejected, like non-gain-switching ones, and they are rejected by both criteria. For this laser, the exclusion areas of both criteria resemble each other except for some outliers in the upper right region which are caused by fluctuations of the autocorrelation values depicted in Figure 4.

The mentioned fluctuations get more and more relevant for the rejection of measurements the lower the boundary is chosen but they are not problematic. All they mean is that in order to produce good random numbers, some measurement sets should be discarded if their autocorrelation is too high. Too low of a driving current leads to the rejection of measured values. The optical output during the on-phases must be high enough to produce a good signal-to-noise ratio (SNR), otherwise the arcsine intensity distribution gets buried under the system noise and no phase randomization can be inferred from the smeared-out histogram. This effect is most prominent in Laser 2 which has lower optical output power compared to the other models. In Figure 9, one can see the effect, namely that data generated by Laser 2 is only accepted when driving the laser at very high currents. This also means that just surpassing the threshold current is not sufficient, a certain overshoot depending on the system is necessary to pass the test.

At too short duty cycles, the criteria are not fulfilled as well. The reason for that are the highly fluctuating relaxation oscillations present at the beginning of the square pulses, causing multi-mode operation and other non-desired effects for interference measurements [24]. Approaching GHz modulation speeds, these oscillations decaying in the order of ns [25] play an important role. If the pulses become too short, one can only measure intensities at points where these oscillations are still dominating. The comparison in Figure 5 shows that the obtained intensity histograms depend heavily on the point of extraction within the pulse. Although a shorter duty cycle should lead to even better phase randomization as the off-time is longer, the data obtained does not guarantee underlying uniform phase distribution as no arcsine distribution is obtained. In order to enable a higher random number generation speed, these relaxation oscillations should be suppressed. This works e.g. by injecting light into the cavity [26] which might have negative effects on the phase randomization dynamics. Another approach to mitigate the influence of these relaxation oscillations connected with chirp of the laser light is to use spectral filters as suggested in [16].

Another temporal behavior was observed through the analysis of the two criteria. Comparing the three lasers in terms of acceptance at various duty cycle values, Laser 1 was found to be unable to produce any accepted data at a duty cycle of DC $= 29/30$ which corresponds to an off-time of 0.17 ns. At the second largest value of DC $= 26/30$ corresponding to an off-time of 0.67 ns some successful measurements were obtained. So, it stops generating random numbers somewhere between these val-

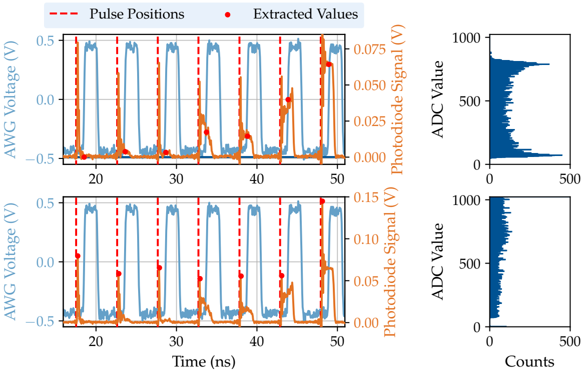

FIG. 5. Pulse trace details from measurements with Laser 3. Top: The data points extracted after the relaxation oscillation regime give a arcsine-like distribution. Bottom: Taking the values in the relaxation oscillation period of the same pulses does not give a proper intensity distribution. The effect of the relaxation oscillation needs to be mitigated at high modulation frequencies.

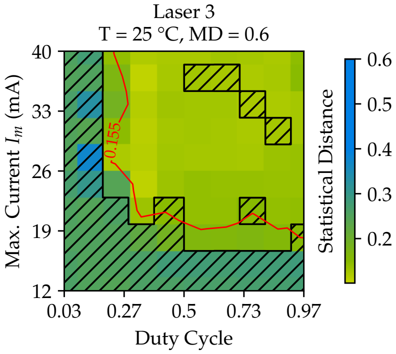

FIG. 6. Visual evaluation of the statistical distance and autocorrelation criteria for a given operating parameter plane for Laser 3. Temperature and modulation depth are fixed, the pulse current and duty cycle are varied. The statistical distance criterion is fulfilled below the boundary of 0.155 indicated by the red line, the autocorrelation is sufficient for parameters which are not shaded. The excluded points in the top right are caused by autocorrelation fluctuations. Such measurement data must be discarded.

ues. Pulsing with an an off-time of 0.5 ns, a value between those two settings, with duty cycle 0.5, one would end up with a pulse frequency of around 1 GHz where the laser begins to fail. The reason for that was found by comparing the measurements to simulations of the experiment. Those simulations were performed with the rate equation model developed in [27] and the laser parameter extraction for it followed the procedure described in [21, 28]. The numerical method described in [25] was used to simulate the rate equations. The experimental result could be reproduced in the simulations by applying a lowpass filter to the input current signal, suggesting that the electronics of the laser bias-T are responsible for the speed limit. Measurements of the amplitude modulation response also confirmed that by showing a sharply decreasing modulation response at a frequency of 1 GHz. The datasheet of the bias-T obtained from the manufacturer indeed stated that there is a modulation limit at 1 GHz. This shows that the developed criteria reflect the capabilities of the QRNG device in terms of its modulation behavior.

As mentioned above, the fluctuations in autocorrelation are substantial and in the order of several dB. For index 1 in Figure 4, calculated from 100 measurements at the same parameter setting, the mean of the gain-switching data is $\overline{\Gamma_1} = -20.8\,\text{dB}$ but the standard deviation ranges from $\Gamma_{1,min} = -26.8\,\text{dB}$ to $\Gamma_{1,max} = -18.4\,\text{dB}$, therefore some measurements overshooting the boundary have to be expected. The mean and standard deviation of the statistical distance calculated from the same measurements at $T = 25\,°\text{C}$, $I_m = 33.78\,\text{mA}$, MD $= 0.51$, and DC $= 0.57$ are $\overline{d_{stat}} = 0.129$ and $\sigma_{d_{stat}} = 0.004$. This deviation is in perfect agreement with the fluctuation simulation result presented in Figure 3. It can become relevant at operating conditions close to the statistical distance boundary, therefore parameters far enough from the boundary should be used for stable operation of the QRNG. The parameter combination used to quantify this deviation, where the fluctuations of the statistical distance do not cause the dismiss of any extracted numbers, constitute an exemplary set of such parameters.

Studying the behavior of the criteria with respect to single varying parameters, the following additional trends are observed. First, the statistical distance decreases above the laser threshold and continues to decrease with increasing pulse current amplitude under gain-switching conditions. This is shown in Figure 7. Improving the SNR is therefore considered to be the best way to improve the statistical quality of the QRNG. The autocorrelation behavior also shows a drop as soon as the signal surpasses the noise but does not decrease much further with increased noise. For the modulation depth there is no further improvement above a certain value, so a certain minimum must be guaranteed. Also for the duty cycle there is a certain threshold to overcome to reach pulse lengths exceeding the relaxation oscillation regime to reach a low statistical distance plateau.The pulse frequency limits for the lasers in terms of the minimum off-time required for phase-randomization could not be explored with the used setup. One would expect a gradual change in both criteria as soon as the phase diffusion width decreases below a certain value.

V. CONCLUSION

A comprehensive evaluation framework for QRNG devices utilizing semiconductor laser phase noise was introduced. The established criteria effectively differentiate

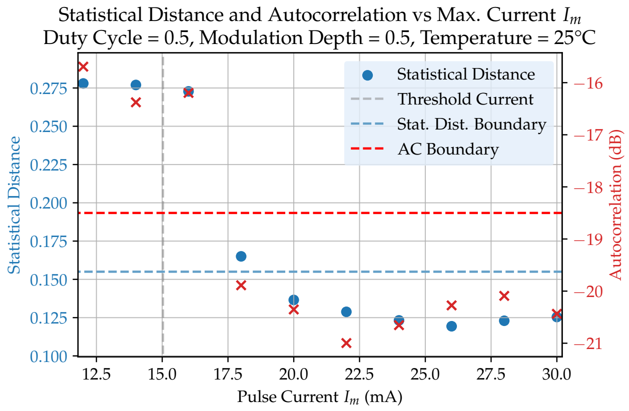

FIG. 7. The statistical distance starts to decrease above the threshold current as the SNR improves. This happens gradually as the arcsine distribution is getting more and more prominent with the overlaying noise staying constant. The autocorrelation drops sharply to values below the boundary above a certain driving current as randomization does not happen gradually when varying the driving current.

between secure and insecure output conditions based on the analyis of phase randomization and autocorrelation. The plausibility of the used criteria could be confirmed by the presented exemplary measurements. The developed tests are applicable for assessing QRNG quality in custom-built devices as required. It is crucial to emphasize that while the statistical randomness evaluated is vital for a dependable random number generator, true security necessitates further examination to prevent potential compromises by malicious entities. This responsibility lies with the operator. Furthermore, this testing suite does not assess the amount of extractable quantum randomness from the output, which requires comprehensive analyses of all classical noise sources. This task is challenging or potentially unfeasible due to the incomplete knowledge of all contributing sources, with the recent identification of phase-locking highlighting a new area of investigation [17]. Nevertheless, our framework introduces a solid qualification routine which can be used by QRNG developers when selecting a suitable laser for their platform.

VI. ACKNOWLEDGEMENTS

The work reported in this manuscript was performed within the QuNET project, funded by the German Federal Ministry of Education and Research under the funding code 16KIS1265. The authors are responsible for the content of this publication.

Appendix A: Comparative Analysis of Laser Performance in Quantum Random Number Generation (QRNG)

1. Observations

The qualification measurements of the three laser models gave insights into their suitability for QRNG applications. It was found that all three lasers can meet the required statistical distance and autocorrelation criteria under specific operating conditions, but their performance varies significantly. This section provides a short comparison of their behaviors, emphasizing their strengths and weaknesses in generating high-quality random numbers.

The absolute minimum statistical distance values achieved by the three lasers are as follows: $d_{stat,min} = 0.103$ for Laser 1, 0.125 for Laser 2, and 0.101 for Laser 3. These results indicate that the outputs of lasers 1 and 3 are closer to the ideal arcsine distribution under optimal conditions. The higher statistical distance for Laser 2 laser is caused by its comparatively low optical output power, leading to a lower SNR and distorting the intensity distribution.

The statistical distance and autocorrelation criteria exclude similar parameter regions for lasers 1 and 3, as shown in Figures 8 and 9. For Laser 2, the overlap is weaker, likely due to its susceptibility to noise. This lase would need a loosened statistical distance boundary condition or reduced detection noise to meet both criteria in a wider window within its possible range of operating conditions, highlighting the need for tailored system design.

All lasers fail to meet the criteria at DC $= 1/30$ (pulses shorter than 0.67 ns) due to relaxation oscillations destabilizing phase and intensity. This causes Gaussian-like distributions instead of the desired arcsine, as illustrated in Figure 5. At DC $= 29/30$ (0.17 ns off-time), Laser 1 cannot operate due to modulation limitations, while both both other models succeed at these DCs.

At high DCs, models 2 and 3 need a minimum MD to lower the off-time driving current or even reverse bias the laser during that time, accelerating cavity field decay and phase diffusion, seen in Figure 10. As stated above, the modulation bandwidth of laser module 1 is limited so that it does not meet the requirements at extreme DCs.

Increasing the chip temperature raises the threshold currents of the lasers, reducing the required modulation depth for gain-switching. This trend is observed in all three lasers, validating the statistical distance boundary as a proxy for laser dynamics.

2. System Limitations and Practical Considerations

Laser 1's default Bias-T limits its modulation to 1 GHz, making it unsuitable for high-speed QRNG application. As mentioned previously, rate equation simula-

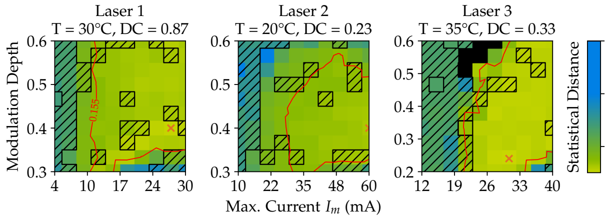

FIG. 8. Three plots showing a certain plane in the parameter space of each laser. Constant parameters are given below the manufacturer title. For each laser, a parameter space plane containing the minimum statistical distance value achieved in the measurements is shown. The minimum values are indicated by the orange cross markers. The black squares represent measurement parameters where the fitting of the arcsine did not work, so that a statistical distance of $d_{\rm stat} = 1$ was obtained.

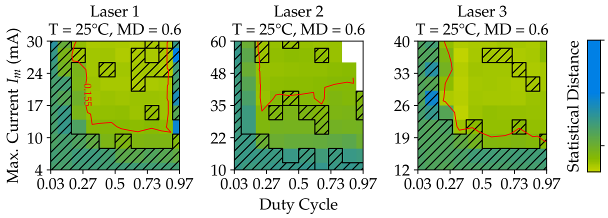

FIG. 9. The statistical distance values plotted on the parameter planes spanned by the pulse peak current and the duty cycle parameters. At very low duty cycles, where the pulses are very short, the lasers do not produce accepted ouput. If only the first part of the pulse is used for interference, where the phase is unstable due to the strong relaxation oscillations, the retrieved distribution is not an arcsine. In that region, typical values of $d_{\rm stat} \approx 0.256$ are achieved with Laser 3, for example. Laser 1 shows insufficient randomization when the duty cycle approaches the maximum achievable value of DC $= 29/30$. An application of Laser 1 for pulse frequencies above 1 GHz is not recommended.

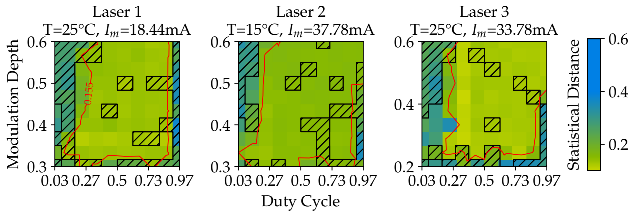

FIG. 10. Statistical distance of measurements taken at constant temperatures and maximum currents. At very low duty cycles the statistical distance criterion is not fulfilled and at very high duty cycles a certain minimum modulation depth is necessary to achieve good operating conditions. This behavior shows that at high modulation speeds, it is important to lower the off-time bias current or even reverse bias the laser in this phase. This decreases the cavity field faster, leading to faster phase randomization.

tions hinted and the manufacturer confirmed that this is an electronics issue, not the laser chip itself. Therefore, the limitation only holds for the specific electronics setup used. The other two models do not show this speed limitation. The performance of Laser 2 is highly sensitive to detection noise, which can obscure the arcsine distribution. This underscores the need for a noise-optimized detection system tailored to the laser. Lasers 1 and 3 on the other hand demonstrate robustness to the noise of the system.

Laser 3 offers the best statistical distance and high duty cycle tolerance, making it ideal for high-speed QRNG applications even with non-optimized detection systems. Laser 1 is suitable for moderate-speed applications but is limited by its modulation electronics at high frequencies. Laser 2 requires careful system design to mitigate the influence of detection noise but can achieve QRNG operation at high duty cycles if these constraints are addressed. For practical QRNG implementation, the choice of laser should balance statistical performance, modulation capabilities, and the influence of the system noise. Continuous monitoring of the statistical distance and the autocorrelation is essential to ensure compliance with defined security requirements for all lasers.

[1] J. E. Gentle, W. K. Härdle, and Y. Mori, eds., *Handbook of computational statistics: Concepts and methods*, 2nd ed., Springer handbooks of computational statistics (Springer, Berlin, 2012).

[2] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications, National Institute of Standards and Technology 10.6028/NIST.SP.800-22r1a (2010).

[3] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, A fast and compact quantum random number generator, Review of Scientific Instruments **71**, 1675 (2000).

[4] J. G. Rarity, P. Owens, and P. R. Tapster, Quantum random-number generation and key sharing, Journal of Modern Optics **41**, 2435 (1994).

[5] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, True random numbers from amplified quantum vacuum, Optics Express **19**, 20665 (2011).

[6] J. Yang, M. Wu, Y. Zhang, J. Liu, F. Fan, Y. Li, W. Huang, H. Wang, Y. Pan, Q. Su, Y. Bian, H. Jiang, J. Dou, S. Yu, B. Xu, and B. L. H. Guo, An ultra-fast quantum random number generation scheme based on laser phase noise (2023).

[7] C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Quantum entropy source on an inp photonic integrated circuit

for random number generation, Optica **3**, 989 (2016).

[8] T. Roger, T. Paraiso, I. De Marco, D. G. Marangon, Z. Yuan, and A. J. Shields, Real-time interferometric quantum random number generation on chip, JOSA B **36**, B137 (2019).

[9] D. G. Marangon, P. R. Smith, N. Walk, T. K. Paraïso, J. F. Dynes, V. Lovic, M. Sanzaro, T. Roger, I. de Marco, M. Lucamarini, Z. Yuan, and A. J. Shields, A fast and robust quantum random number generator with a self-contained integrated photonic randomness core, Nature Electronics **7**, 396 (2024).

[10] X. Guo, F. Lin, J. Lin, Z. Song, Y. luo, Q. Wang, and Y. Guo, *Parallel and real-time post-processing for quantum random number generators* (2024).

[11] Q. Li, X. Sun, X. Zhang, and H. Zhou, Improved real–time post–processing for quantum random number generators, Advanced Quantum Technologies **7**, 2400025 (2024).

[12] C. Henry, Phase noise in semiconductor lasers, Journal of Lightwave Technology **4**, 298 (1986).

[13] B. Septriani, O. de Vries, F. Steinlechner, and M. Gräfe, Parametric study of the phase diffusion process in a gain-switched semiconductor laser for randomness assessment in quantum random number generator, AIP Advances **10**, 10.1063/5.0011418 (2020).

[14] Y. Dodis, V. Vaikuntanathan, and D. Wichs, Extracting randomness from extractor-dependent sources, in *Advances in Cryptology – EUROCRYPT 2020*, Springer eBook Collection, Vol. 12105, edited by A. Canteaut and Y. Ishai (Springer International Publishing and Imprint Springer, Cham, 2020) pp. 313–342.

[15] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode, Optics express **22**, 1645 (2014).

[16] R. Shakhovoy, V. Sharoglazova, A. Udaltsov, A. Duplinskiy, V. Kurochkin, and Y. Kurochkin, Influence of chirp, jitter, and relaxation oscillations on probabilistic properties of laser pulse interference, IEEE Journal of Quantum Electronics **57**, 1 (2021).

[17] R. Shakhovoy, E. Maksimova, M. Boltanskiy, and M. Fadeev, Influence of optical self-injection on statistical properties of laser-pulse interference (2025).

[18] P. R. Smith, D. G. Marangon, M. Lucamarini, Z. L. Yuan, and A. J. Shields, Out-of-band electromagnetic injection attack on a quantum random number generator, Physical Review Applied **15**, 10.1103/PhysRevApplied.15.044044 (2021).

[19] M. Rudé, C. Abellán, A. Capdevila, D. Domenech, M. W. Mitchell, W. Amaya, and V. Pruneri, Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources, Optics express **26**, 31957 (2018).

[20] M. W. Mitchell, C. Abellan, and W. Amaya, Strong experimental guarantees in ultrafast quantum random number generation, Physical Review A **91**, 10.1103/PhysRevA.91.012314 (2015).

[21] V. Lovic, D. G. Marangon, M. Lucamarini, Z. Yuan, and A. J. Shields, Characterizing phase noise in a gain-switched laser diode for quantum random-number generation, Physical Review Applied **16**, 10.1103/PhysRevApplied.16.054012 (2021).

[22] T. Kobayashi, A. Tomita, and A. Okamoto, Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser, Physical Review A **90**, 10.1103/PhysRevA.90.032320 (2014).

[23] Z. Gajić, *Linear dynamic systems and signals* (Pearson Education, Upper Saddle River, NJ, 2003).

[24] T. Numai, *Fundamentals of Semiconductor Lasers*, 2nd ed., Springer Series in Optical Sciences Ser, Vol. v.93 (Springer Japan, Tokyo, 2015).

[25] T. K. Paraïso, R. I. Woodward, D. G. Marangon, V. Lovic, Z. Yuan, and A. J. Shields, Advanced laser technology for quantum communications (tutorial review), Advanced Quantum Technologies **4**, 10.1002/qute.202100062 (2021).

[26] R. Lang and K. Kobayashi, Suppression of the relaxation oscillation in the modulated output of semiconductor lasers, IEEE Journal of Quantum Electronics **12**, 194 (1976).

[27] J. E. Bowers, High speed semiconductor laser design and performance, Solid-State Electronics **30**, 1 (1987).

[28] J. C. Cartledge and R. C. Srinivasan, Extraction of dfb laser rate equation parameters for system simulation purposes, Journal of Lightwave Technology **15**, 852 (1997).